час на виконання рутинних операцій завдяки автоматизації. Результати тестування функціональних вимог підтвердили працездатність і відповідність системи специфікаціям, що засвідчує її готовність до практичного використання. У подальших дослідженнях планується розширення функціональних можливостей застосунку, зокрема додавання аналітичних звітів, інтеграція з інструментами штучного інтелекту для прогнозування термінів виконання задач і підтримка багатомовного інтерфейсу.

Список використаних джерел

1. Кондратьєв Олександр. Розроблення вебзастосунку для управління завданнями та проєктами з метою оптимізації процесів проєктного менеджменту / О. Кондратьєв // Матеріали Міжнародної науково-практичної конференції молодих учених, аспірантів та студентів “Інформаційні технології в сучасному світі: дослідження молодих вчених”: тези доповідей, 27–28 лютого 2025 р. – Х. : ХНЕУ імені Семена Кузнеця, 2025. – с. 4.2.

2. Як створити бекенд за допомогою Supabase [Електронний ресурс] / Академія кодування // YouTube. codeacademyua. – Електрон. відеодан. – Режим доступу : https://www.youtube.com/watch?v=ae2Eaz_zEqO

3. Project Management Institute – Learn about project management standards and certifications [Електронний ресурс] // PMI. – Режим доступу : https://www.pmi.org .

УДК 621.317

Скорін Юрій
кандидат технічних наук, доцент
Харківський національний економічний університет ім. С. Кузнеця
Лактіонов Артем
студент
Харківський національний економічний університет ім. С. Кузнеця

ГІБРИДНІ МЕТОДИ ШИФРУВАННЯ У БЛОКЧЕЙН-МЕРЕЖАХ

Метою проведеного дослідження є впровадження гібридних методів шифрування для забезпечення конфіденційності, цілісності та автентичності переданих даних у блокчейн-мережах. Було проаналізовано сучасні криптографічні алгоритми, виявлено їхні переваги та недоліки, а також запропоновано гібридну схему, яка поєднує симетричне та асиметричне шифрування. Об’єктом дослідження є процес обміну даними між учасниками блокчейн-мережі. Предметом дослідження є криптографічні методи, орієнтовані на підвищення безпеки передачі інформації. Було проведено аналіз криптографічних ризиків, виявлено типові вразливості передачі даних у публічних блокчейнах, зокрема при обміні ключами та передачі конфіденційної інформації до або поза межами мережевого консенсусу. Результатом

проведеного дослідження є розроблення рішення захищеного каналу передачі даних з використанням гібридного шифрування, що адаптований до особливостей блокчейн-середовища.

У сучасних інформаційних системах питання, які пов'язані з забезпеченням кібербезпеки набуває ключового значення. Зі зростанням обсягів цифрових транзакцій, популярністю децентралізованих застосунків та використанням блокчейн-технологій у різних сферах (логістика, фінанси, охорона здоров'я, ідентифікація тощо) зростає і потреба в надійних методах захисту переданої інформації. Хоча сам блокчейн забезпечує цілісність і незмінність записів у розподіленому реєстрі, він не гарантує повної конфіденційності та автентичності переданих даних, особливо в каналах взаємодії між користувачами або вузлами мережі. Передавання інформації в блокчейн-середовищах часто відбувається без додаткових рівнів шифрування або з використанням застарілих алгоритмів. Це створює загрозу перехоплення, несанкціонованого доступу або навіть модифікації критично важливої інформації. Використання лише симетричних або лише асиметричних алгоритмів не завжди є ефективним через компроміс між продуктивністю та рівнем безпеки. Одним із перспективних напрямів вирішення цих проблем є впровадження гібридних методів шифрування, які поєднують переваги симетричних (висока швидкодія) та асиметричних (безпечний обмін ключами) криптографічних систем. Такий підхід дозволяє забезпечити як швидке кодування інформації, так і захищений обмін ключовими параметрами, що особливо актуально у відкритих або частково відкритих блокчейн-мережах.

Метою проведеного дослідження є обґрунтування та розроблення гібридної криптографічної схеми, адаптованої для захищеного передавання даних у блокчейн-мережах. Об'єктом дослідження є процес передавання цифрових даних у децентралізованих обчислювальних системах. Предметом дослідження виступають методи симетричного та асиметричного шифрування, їх комбіноване застосування в умовах розподіленого середовища. У якості методів дослідження задіяні такі методи, як теоретичний аналіз криптографічних протоколів, моделювання процесів шифрування, проєктування захищених схем, експериментальна оцінка продуктивності. Практичне значення проведеного дослідження полягає у поєднанні сучасних криптографічних підходів в одну ефективну гібридну модель, що враховує особливості функціонування блокчейн-мереж.

У сучасному інформаційному просторі блокчейн-технології активно впроваджуються в різноманітні галузі – від фінансового сектора й логістики до освіти, охорони здоров'я та державного управління. Основною перевагою блокчейну є забезпечення цілісності, прозорості та незмінності інформації, що зберігається у розподіленому реєстрі. Водночас, попри поширену думку про високий рівень безпеки децентралізованих систем, блокчейн сам по собі не забезпечує повноцінного захисту переданої інформації, особливо на рівні комунікації між учасниками мережі. Актуальними залишаються загрози, властиві класичним комп'ютерним мережам: атаки типу «людина посередині», які дозволяють втручатися у передавання даних між вузлами; підміна

транзакцій або маніпуляція з вмістом до моменту їхнього включення у блок; перехоплення приватної інформації у процесі створення, підписання чи передачі транзакцій; експлуатація слабких або застарілих алгоритмів криптографії, що не відповідають сучасним стандартам. Крім того, у блокчейн-мережах часто використовуються відкриті ключі для ідентифікації користувачів, тоді як відповідні приватні ключі зберігаються локально. Втрата чи компрометація приватного ключа призводить до безповоротної втрати доступу або повного контролю над обліковим записом, що підтверджує необхідність додаткових рівнів захисту. Особливої уваги вимагає проблема конфіденційності у блокчейн-середовищах. Наприклад, у фінансових додатках або децентралізованих біржах транзакції містять дані про суми, адреси сторін, хеші контрактів тощо. Якщо така інформація буде доступною стороннім особам, це може призвести до витоку комерційної або персональної інформації. Низка досліджень показує, що частина блокчейн-застосунків (особливо у сфері охорони здоров'я, цифрової ідентифікації, корпоративного документообігу) потребує не лише збереження цілісності даних, а й забезпечення їхньої конфіденційності. Однак стандартні механізми більшості публічних блокчейн-платформ цього не передбачають. У той час як протоколи рівня TLS або HTTPS забезпечують захист каналу у класичних мережах, у блокчейні подібний захист має бути реалізований самостійно, на рівні застосунку або через спеціалізовані криптографічні схеми. Одним із можливих рішень для підвищення безпеки передачі інформації у таких мережах є застосування гібридного шифрування. Воно дозволяє забезпечити шифрування самого вмісту повідомлення за допомогою симетричних алгоритмів (наприклад, AES), а також здійснити захищений обмін ключами за допомогою асиметричних алгоритмів (наприклад, ECC або RSA). Такий підхід забезпечує не лише конфіденційність і автентичність, а й підвищує ефективність у децентралізованих мережах з великою кількістю учасників.

Таким чином, попри сильні сторони блокчейн-архітектури у забезпеченні незмінності й верифікованості інформації, уразливості, пов'язані з конфіденційністю та захищеністю каналів передачі даних, залишаються актуальними. Це формує необхідність впровадження додаткових криптографічних засобів – зокрема, гібридних методів шифрування, що дозволяють комплексно підвищити рівень інформаційної безпеки в блокчейн-мережах. В умовах швидкого розвитку децентралізованих технологій зростає потреба в оцінці не лише функціональної, але й прикладної ефективності засобів захисту інформації. Для блокчейн-систем, де кожна транзакція є публічною, а структура мережі не передбачає централізованих елементів безпеки, надзвичайно важливою є здатність обраної криптографічної моделі забезпечувати надійний захист переданої інформації без шкоди для продуктивності, доступності та сумісності з наявними протоколами.

У зв'язку з цим доцільно провести комплексний аналіз ефективності гібридної моделі шифрування, яка була досліджена у попередніх розділах, та визначити її переваги, обмеження і перспективи використання в сучасних блокчейн-інфраструктурах. Аналіз показав, що найбільш ресурсоємними

етапами є генерація асиметричних ключів та обчислення спільного секрету, що очікувано. Проте загальна затримка залишається в межах допустимого навіть для інтерактивних DApp або мобільних застосунків. Було проведено порівняння гібридної моделі з іншими методами, які використовуються у криптографії (тільки симетричне або тільки асиметричне шифрування), за ключовими параметрами. Ці результати підтверджують, що гібридна модель забезпечує найкращий баланс між безпекою і продуктивністю, особливо в умовах, де необхідно забезпечити захищений обмін ключами та цілісність повідомлень у відкритій децентралізованій мережі.

У результаті тестування, порівняння та аналітичного аналізу було підтверджено, що гібридна криптографічна модель має високу практичну цінність у контексті підвищення інформаційної безпеки передачі даних у блокчейн-мережах. Вона демонструє ефективну комбінацію криптографічної надійності, продуктивності, гнучкості впровадження та відповідності майбутнім викликам (зокрема квантовим загрозам).

У ході виконання курсової роботи було проведено комплексне дослідження гібридних методів шифрування та їх застосування для забезпечення захисту інформації у блокчейн-середовищах. Метою роботи було дослідити принципи побудови та функціонування гібридних криптографічних систем, проаналізувати їхні переваги у порівнянні з традиційними методами шифрування, а також оцінити доцільність та ефективність їх інтеграції в інфраструктуру блокчейн-технологій. На основі проведеного теоретичного аналізу було встановлено, що гібридна криптографія поєднує у собі сильні сторони як симетричних, так і асиметричних методів шифрування: високу швидкодію симетричних алгоритмів (зокрема AES) та безпечну передачу ключів, яку забезпечують асиметричні алгоритми (наприклад, ECC). Така комбінація дозволяє досягти оптимального балансу між продуктивністю та безпекою в умовах децентралізованих мереж. У практичній частині було проаналізовано інструментальні засоби реалізації гібридного шифрування, зокрема бібліотеку PyCryptodome, яка продемонструвала високу функціональність та відповідність сучасним вимогам інформаційної безпеки. Було змодельовано сценарії шифрування, обміну ключами, верифікації цілісності повідомлень та проведено аналіз продуктивності алгоритмів.

Результати дослідження продемонстрували високу ефективність обраної криптографічної моделі: низькі затримки при шифруванні й дешифруванні, підтримка сучасних стандартів, придатність до масштабування та захист від основних типів атак (включно з MITM та аналізом трафіку). Порівняльна оцінка також підтвердила переваги гібридної моделі перед класичними підходами. Таким чином, отримані результати є основою для розробки практичних рішень у сфері безпечного передавання даних у Web3-системах, децентралізованих застосунках та цифрових екосистемах нового покоління.

Список використаних джерел

1. ДСТУ 3008:2015 Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. – Київ : ДП УкрНДНЦ, 2015. – 28 с.

2. ДСТУ 3582:2013. Інформація та документація. Бібліографічний опис. Скорочення слів і словосполучень українською мовою. Загальні вимоги та правила (ISO 4:1984, NEQ; ISO 832:1994, NEQ) / Нац. стандарт України. – Київ : Мінекономрозвитку України, 2014. – 18 с.

3. ДСТУ 8302:2015. Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання / Нац. стандарт України. – Київ : ДП «УкрНДНЦ», 2016. – 18 с.

4. Шифрування. Типи і алгоритми [Електронний ресурс]. – Режим доступу: https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/.

5. Шифрування: типи і алгоритми. Що це, чим відрізняються і де використовуються [Електронний ресурс]. – Режим досутпу: https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/.

6. Порівняння симетричного і асиметричного шифрування [Електронний ресурс]. – Режим досутпу: https://exbase.io/uk/wiki/simetrichne-i-asimetrichne-shifruvannya.

УДК 621.317

Скорін Юрій
кандидат технічних наук, доцент
Харківський національний економічний університет ім. С. Кузнеця
Лук'янчук Софія
студентка
Харківський національний економічний університет ім. С. Кузнеця

ШТУЧНИЙ ІНТЕЛЕКТ В СИСТЕМАХ УПРАВЛІННЯ ФІНАНСОВИМИ РИЗИКАМИ

Метою проведеного дослідження є застосування штучного інтелекту в автоматизованих системах управління фінансовими ризиками з метою підвищення точності, оперативності та ефективності прийняття управлінських рішень у фінансовій сфері. У межах дослідження розроблено модель прогнозування кредитного ризику клієнтів банку, яка дозволяє здійснювати оцінку платоспроможності на основі історичних даних та сучасних методів машинного навчання. Об'єктом дослідження є автоматизовані системи управління фінансовими ризиками, які функціонують у банківському та фінансовому секторі. Предметом дослідження виступають алгоритми та моделі штучного інтелекту, які можуть бути інтегровані до автоматизованих систем управління фінансовими ризиками з метою підвищення точності прогнозів та